Theory of risks and processing of medical data in Healthgrids in European Law

Herveg, Jean

Published in:
La protection des données médicales. Les défis du XXIe siècle - The protection of medical data. Challenges of the 21st century

Publication date:
2008

Document Version
Publisher's PDF, also known as Version of record

Theory of risks and processing of medical data in Healthgrids in European Law [1]

Jean HERVEG
Lecturer, Faculty of Law (FUNDP)
Research Centre on IT and Law (CRID), FUNDP, Namur
Member of the Bar of Brussels

Introduction

1. The introduction of Grid technologies in healthcare arouses numerous legal questions [2]. Among these, one is to know how are managed the risks created by the underlying processing of medical data occurring in Healthgrids, with respect to the rights and freedoms of the data subject. With this end in view, the paper investigates the management of risks in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [3].

This work benefits from the support of several projects: SHARE (Supporting and Structuring HealthGrid Activities & Research in Europe: Developing a Roadmap) (Specific Support Action, FP6-2005-IST-027694), ACGT (Advancing Clinico-Genomics Trials on Cancer: Open GRID Services for Improving Medical Knowledge Discovery) (Integrated Project, FP6-2005-IST-026996), WALIBI (Wireless Acquisition and LInk for Body Information) (convention Région wallonne n° 616449). The views expressed in the paper engage only their author.

For a first overview on these legal issues: J. HERVEG & Y. POULLET, "Healthgrid from a Legal Point of View", in *From GRID to HEALTHGRID*, Studies in Health Technology and Informatics, vol. 115, part 5, IOS Publications, 2005, p. 312-218.

Journal officiel des Communautés européennes, n° L 281, 23 Nov. 1995, p. 31-50. For an in-depth analysis of the Directive: Y. Poullet, M.-H. Boulanger, C. de Terwangne, Th. Leonard, S. Louveaux & D. Moreau, "La protection des données à caractère personnel en droit communautaire", *Journal des Tribunaux de droit européen*, Brussels, Larcier, 1997, p. 121 et s. (in three parts). The analysis of the protection of personal data is supported by the opinions issued by the Data Protection Working Party (art. 29 of Directive 95/46/EC). This directive

I. 'Theory of risks' in Directive 95/46/EC

2. European Directive 95/46/EC pursues a double objective when harmonising the national legislations of the European Member States. It aims at the free movement of personal data, asserted as necessary to the creation and the operating of the Common Market [4], and for the protection of fundamental rights and freedoms of natural persons concerned by the personal data [5] (the data subject), and in particular their right to privacy with respect to the processing of personal data [6].

In order to remove the obstacles to the free movement of personal data in the Common Market, it was of prime importance to harmonise national legislations, so that all Member States offer an equal but high level of protection towards the rights and freedoms of persons regarding the processing of personal data [7]. After such harmonisation, the Member States may not prevent anymore the free movement of personal data for reasons relative to the protection of natural persons' rights and freedoms, including the right to respect for private life. As the harmonisation is limited in its material scope, the Member States may restrict the free movement of personal data for other reasons than those relative to the protection of natural persons' rights and freedoms [8] – without prejudicing the application of articles 95.8 and 95.10 of the Treaty creating the European Community or of any other rules opposing any restriction to the free movement of personal data within Member States or the Common Market.

3. Having in mind the establishment of this legal framework in all European Member States (although this framework is relatively incomplete in a sense), the Directive is the result of a quantitative and qualitative assessment of the risks which the personal data processing may cause to the data subjects' rights and freedoms.

Indeed, to be effective and coherent, this protection requires the knowledge of the risks capable to affect the fundamental rights and freedoms of the data subject. It is only possible to determine the conditions under which personal data can be processed in full respect of the fundamental rights and freedoms of data subjects if these risks are identified.

4. This assessment has been realised to all levels of the Directive's scope.

The Directive determines its material scope (cf. Chapter 1 of the Directive) [9]. It focuses only on situations which require some protection. The latter implies to estimate the risks for the data subjects' rights and freedoms. For example, the Directive only applies to the completely or partially automated processing [10] of personal data [11] and to the non-automated processing of personal data figuring or aiming to figure in a filing system [12]. However, the Directive does not apply to the processing

derives from the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Council of Europe, European Treaty Series, n° 108, Strasbourg, 28 Jan. 1981). See also: Regulation (EC) No. 45/2001 on the protection of individuals with regard to the processing of personal data by the Community, institutions, and bodies, and on the free movement of such data; Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications); Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. From the European Court of Justice: E.C.J., 29 January 2008, Productores de Musica de Espana (Promusicae) v. Telefonica de Espana SAU, Case C-275/06; E.C.J., 30 May 2006, European Parliament v. Council of the European Union and Commission of the European Communities, Joined Cases C-317/04 and C-318/04); E.C.J., 6 November 2003, Bodil Lindqvist v. Sweden, case C-101/01; E.C.J., 20 May 2003, Rechnungshof v. Österreichischer Rundkunf and Others and Christa Neukomm and Joseph Lauermann v. Österreichischer Rundfunk, Joined Cases C-465/00, C-138/01 and C-139/01. Two cases from the Court of First Instance present some interest: C.F.I., 8 November 2007, Bavarian Lager v. Commission of the European Communities, Case T-194/04; C.F.I., 12 September 2007, Kalliopi Nikolaou v. Commission of the European Communities, Case T-259/03. On the other hand, the Council of the Organisation for Economic Co-operation and Development (OECD) has adopted Recommendation concerning guidelines governing the protection of privacy and transborder flows of personal data on 23 September 1980. The High Commission for Human Rights has adopted Guidelines for the Regulation of Automated Files containing Personal Data on 14 December 1990. A special mention has to be done to Article 8 of the European Convention on Human Rights (and to its jurisprudence from the European Court of Human Rights and notably to the cases of Z c. Finland (25 Febr. 1997) and M.S. c. Sweden (27 Aug. 1997) and to the Recommendation adopted by the Council regarding the protection of medical data (Rec n° R (97)5, 13 Feb. 1997).

4. Directive 95/46/EC, art. 1.2, and recitals 3, 4, 5, 6, 7, 8 and 9.
5. Directive 95/46/EC, recitals 2, 3, 10 and 11.
6. Directive 95/46/CE, art. 1.1.
7. Directive 95/46/EC. recital 8. See also art. 1 and recital 9.

8 Like Public Order or Social Security.

9 On Directive 95/46/EC scope: C.J.C.E., 20 May 2003, Rechnungshof & al., C-465/00, C-138/01 and C-139/01; C.J.C.E., 6 Nov. 2003, Bodil Lindqvist, case C-101/01, C. de TERWANGNE, "Affaire Lindqvist ou quand la Cour de justice des Communautés européennes prend position en matière de protection des données personnelles", *Revue du droit des technologies de l'information*, Brussels, Ed. Bruylant, 2004, p. 67-99.

10 'Processing of personal data' ('processing') means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction (Directive 95/46/EC, art. 2.b) (cf. recital 14). See also: Council of Europe, T-PD, Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data (2005); Data Protection Working Party, Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware, WP 17, adopted on 23 February 1999.

11 'Personal data' are any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity (Directive 95/46/EC, art. 2.a). For more details on the notion of personal data and providing an even broader definition, see the (controversial?) Opinion n° 4/2007 on the concept of personal data, adopted on 20th June by the Data Protection Working Party, WP 136. The problem with the latter is to know what could remain as 'non personal' data.

of personal data carried out by a natural person for exclusively personal or domestic reasons [13].

Furthermore, the Directive provides the general conditions for the lawfulness of the personal data processing (cf. Chapter 2 of the Directive).

It requires the existence of judicial remedies for the protection of personal data and creates a special liability upon the data controller, without omitting the question of sanctions in case of infringement of certain rules (cf. Chapter 3 of the Directive).

The Directive also rules the transfer of personal data outside the European Union (cf. Chapter 4 of the Directive) [14].

Finally, the Directive addresses the question of the Codes of Conduct (cf. Chapter 5 of the Directive) and establishes special institutions and bodies, such as the national supervisory authorities, the Working Group on the protection of individuals with regard to the processing of personal data (cf. Chapter 6 of the Directive) and the Committee composed of the Member State Representatives concerning community implementing measures (Committee 31) (cf. Chapter 7 of the Directive).

5. Considered in a global approach, Directive 95/46/EC manages the risks presented by the processing of personal data by means of four steps [15].

In a first step, the Directive determines the legal framework applicable to any processing of personal data (including sensitive data [16]).

In a second step, the Directive provides special rules to legitimate the processing of sensitive data. It goes without saying that the legal framework developed in the first step applies in addition to the processing of sensitive data.

In a third step, the Directive imposes special rules to the processing of personal data presenting specific risks to the data subjects' rights and freedoms. This third approach must also be added to the two previous ones. It is not exclusive of their application for the rest of the data processing.

In a fourth and last step, the Directive regulates the transfers of personal data outside the European Union.

12 Directive 95/46/EC, art. 3.1.

13 Directive 95/46/EC, art. 3.2 (cf. recital 12).

14 Council of Europe, T-PD, Study contracts involving the transfer of personal data between Parties to Convention Ets 108 and third countries not providing an adequate level of protection (2001), by Mr. Jérôme HUET.

15 J. HERVEG, "La gestion des risques spécifiques aux traitements de données médicales en droit européen", in *Systèmes de santé et circulation de l'information, Encadrement éthique et juridique*, Paris, Dalloz, 2006, p. 79-103.

16 Usually, sensitive data are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

6. This risk assessment is particularly important since the recent evolutions of Information and Communication Technologies have multiplied the possibilities to process personal data and therefore increased the risks of infringement to the fundamental rights and freedoms of the data subject.

The use of a new technology such as Healthgrid should naturally induce the assessment of the risks attached to its implementation, especially in healthcare when regarding the protection of medical data.

This paper investigates only the first three steps of this risk assessment.

II. The management of 'ordinary' risks in the processing of personal data

7. The risk management for the data subjects' rights and freedoms relies on a relatively simple principle: the risk does not depend on the informational content of the personal data but on the context in which they will be used [17]. In other words, the risk depends on the purpose pursued by the processing of personal data. Therefore, the potential or real threat from the processing of personal data has to be assessed with regard to the purpose pursued by the data controller.

There lies the reason why personal data consist in any information relative to an identified or identifiable natural person and not only information susceptible to reveal the intimacy of data subjects. Hence, all information, including the more common kind such as a phone number or a number plate, are personal data as long as they are related to an identified or (reasonably) identifiable natural person because the use of this kind of information may expose data subjects to some risks of infringement of their rights and freedoms, including their right to control (in some extent) the use of their personal data, with no regard to any specific informational content of the personal data. The aim of the Directive (the management of the risks presented by any use of information relative to identified or identifiable natural persons) explains for the definition of personal data.

III. The management of 'special risks' in the processing of personal data

8. However, the principle relative to the risk management in the processing of personal data is slightly though not completely different with respect to the processing of 'sensitive' data, the latter including medical data. Indeed, it is common knowledge that the informational content of sensitive data increases the risks of

Convention n° 108, Report, recital 43.

infringement of the data subjects' rights and freedoms, in addition to the risk resulting from the purpose of their processing.

In other words, any operation realised upon sensitive data exposes data subjects to greater risks of infringement of their rights and freedoms [18]. That is the reason why 'sensitive' data require a special protection which has to take into account their informational content as well as the purpose of their processing.

Accordingly, the Directive bans the processing of 'sensitive' data [19] because *"data which are capable by their nature of infringing fundamental freedoms or privacy should not be processed"* [20]. Put otherwise, this ban represents the special protection adopted by the Directive for 'sensitive' data, including medical data. Being prohibited, the processing of 'sensitive' data is no more susceptible to present any risk for the data subjects' rights and freedoms. Somehow, this policy aims to minimise the risks presented by the processing of 'sensitive' data.

Hence, the ban on processing medical data should not be seen as opposed to the free movement of personal data. The ban on processing medical data is more a limit than an exception to the free movement of personal data. In fact, the free movement of personal data can only be conceived in the full respect of the fundamental rights and freedoms of the data subject, and this respect includes the ban on processing medical data.

9. Nevertheless, the Directive provides a number of cases in which the prohibition to process 'sensitive' data does not apply [21]. In these cases, the legitimacy of the processing of 'sensitive' data (their admissibility) is formally presumed. Indeed, these situations are of nature to justify derogation to the prohibition of processing 'sensitive' data without prejudice to the other rules applicable to the processing of personal data. Noteworthy, these exceptions to the prohibition to process 'sensitive' data have to be strictly interpreted. Beyond these exceptions, the processing of 'sensitive' data is not allowed.

In each of these exceptions, the risk presented by the processing of 'sensitive' data is formally presumed to be adequately under control. It must be immediately stressed that these exceptions do not imply an absence of risk, but express the balance of the interests in presence. This requires assessing the risks for the data subjects' rights and freedoms in order to reasonably appreciate the admissibility of the processing of 'sensitive' data.

18 Convention n° 108, Report, recital 43.

19 Directive 95/46/EC, art. 8.1.

20 Directive 95/46/EC, recital 33. Convention n° 108 is not so explicit in its art. 6.

21 Directive 95/46/EC, art. 8. On the ban and its exception, see: J. HERVEG, "The Ban on Processing Medical Data in European Law: Consent and Alternative Solutions to Legitimate Processing of Medical Data in HealthGrid", in *Challenges and Opportunities of HealthGrids*, Studies in Health Technology and Informatics, vol. 120, Amsterdam, IOS Press, 2006, p. 107-116.

10. Accordingly, the Directive grants permission to process medical data [22] in seven hypotheses. Herein the legitimacy of the processing of medical data (the balance between the interests in presence [23]) is formally presumed (cf. *infra* the necessity to really assess its legitimacy). This is explained by the fact that, in principle, the situations described in these hypotheses should justify the processing of medical data, without prejudice for the other conditions ensuring the lawfulness of the data processing. It has to be reminded that these exceptions to the ban on processing medical data should be restrictively interpreted and that the processing of medical data is strictly forbidden beyond these exceptions.

The first hypothesis granting permission to process medical data is the consent of the data subject. The data subject's consent is frequently presented as the natural base for the legitimacy of the processing of medical data, even if it is not (and by far) the only one.

A. The consent of the data subject

11. According to the Directive, the ban on processing medical data does not apply where the data subject has given his or her explicit consent to the processing of medical data [24].

In this case the Directive entrusts the data subject with the power to authorise the processing of medical data [25]. This empowerment of data subject represents without any doubt a very strong expression of his or her informational self-determination – the power of the data subject upon personal data [26].

22 The notion of medical data includes all information relative to any aspect, physical or psychological, of the present, past or future health condition, good or bad, of a living or dead natural person (even if the letter is controversial). On the definition of medical data: Explanatory report of Convention n° 108, recital 45; Rec. (97) 5 of the Council of Europe relative to the protection of medical data, art. 1 of the annex; C.J.C.E., 6 Nov. 2003, Bodil Lindqvist, case C-101/01, C. DE TERWANGNE, o.c., *Revue du droit des technologies de l'information*, Brussels, Ed. Bruylant, 2004, p. 67-99; Groupe européen d'éthique des sciences et des nouvelles technologies, avis n° 13 du 30 juillet 1999 sur les aspects éthiques de l'utilisation des données personnelles de santé dans la société de l'information. See also: Council of Europe, T-PD, Revisiting Sensitive Data (1999), by Mr. Spiros SIMITIS.

23 Cf. *infra* for the identification of these interests.

24 Directive 95/46/CE, art. 8.2. a. The national law may provide that the data subject's consent may not lift the prohibition.

25 Directive 95/46/CE, recital 33.

26 On the notion of informational self-determination: Fr. RIGAUX, *La protection de la vie privée et des autres biens de la personnalité*, Paris, L.G.D.J., Bruxelles, Bruylant, 1990, p. 588-589, n° 532: "(...) La juridiction constitutionnelle a déduit du droit de la personnalité l'un de ses attributs, à savoir: "le pouvoir reconnu à l'individu et résultant de la notion d'auto-détermination, de décider en premier lieu lui-même quand et dans quelle mesure des faits relatifs à sa propre existence sont divulgués (...). Cet attribut du droit de la personnalité est appelé 'droit à la maîtrise des données personnelles' (...). Il n'est toutefois pas sans limite (...)". See also: Council of Europe, Resolution 1165 (1998), 26 June 1998, *Droit au respect de la vie privée* (24th Session), point 5.

But this empowerment might also surprise. Is the data subject always capable to decide in a reasonable way about the processing of medical data? Isn't it too dangerous to give such power to the data subject when most of the time he or she will represent the 'weakest' party or at least the 'demanding' person in the processing of medical data? By example, how could a patient oppose the processing of medical data for scientific purpose (e.g. for a clinical trial) before surgery or any other investigation? How to ensure the validity of the data subject's consent and avoid a complete masquerade?

This empowerment of the data subject should not be seen as unlimited or under no control. In fact, when given this power the data subject has to evaluate the interest(s) that could justify the processing of medical data. With this end in view, the data subject has to put correctly into balance the interests in presence and to act accordingly. Otherwise, the consent will not be able to legitimate the processing of medical data (see *infra* about the necessity to really assers the legitimacy of the processing of medical data and the question of the determination of the interests to take into account).

The Directive confirms this analysis.

12. Regarding the Directive, the data subject's consent means *"any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed"* [27].

First the consent has to be indubitable, indisputable, without any doubt.

Then the consent of the data subject must have been freely given. In this regard, the consent has to be free of any vice, constraint or pressure. With respect to this, any direct profit (such as the benefit for his or her health) or indirect profit (such as the participation to the progress of medical science) for the patient should not affect automatically the validity of the data subject's consent. Would the financial retribution of the data subject (beyond the cover of his or her eventual expenses) invalidate his or her consent? The answer to this question should not be absolute. It should depend upon the circumstances of each considered case and on how the applicable law deals with the protection of the data subject.

Moreover, the consent of the data subject has to be specific and informed. 'To be specific' means that the data subject must know exactly what he or she consents to. The latter implies necessarily the prior and adequate information of the data subject concerning the processing of medical data. Without this prior and adequate information, the consent of the data subject shall not be specific. Therefore, and in any case, the consent of the data subject does not validate the processing of medical data.

27 Directive 95/46/CE, art. 2, h.

In this respect, the next question is logically the determination of the detail level of the information to be delivered to the data subject. Articles 10 and 11 of the Directive determine the minimum content of this information. The latter must permit the complete enforcement of all aspects of the data processing – such as the data quality, the data subject's rights, the security and confidentiality measures, the notification to the supervisory authority, etc. However, there is no doubt that the information has to be more accurate and complete, particularly since very sensitive data as medical data are processed.

In any case, the data subject may not give an unspecified or uninformed consent to the processing of medical data.

Further processing of medical data is prohibited when incompatible with the initial purpose for which data have been collected.

The consent must be given prior to the data collection. It must not be given necessarily at the same time; it only has to be obtained prior to the processing.

13. The consent of the data subject must be explicit to allow for the processing of medical data [28].

A contrario, the requirement of an explicit consent should exclude any implicit consent – whatever this last notion could be. With respect to this, beyond the indisputable character of the data subject's consent, its explicit characteristic presumes that it has been expressed.

Frequently, the signed form including the data subject's consent is viewed as the best complying transposition of this requirement. Several Member States have decided to transpose this requirement by imposing a written consent from the data subject.

However, the explicit consent can be deduced from some other behaviour of the data subject especially regarding the circumstances of the case. Indeed, some positive actions could express the explicit consent of the data subject to the processing of medical data, such as the financial participation to a foundation fighting against the disease affecting the data subject or as the demand to be treated in a special medical unit notoriously known as being a research unit.

14. In all these circumstances, the consent of the data subject induces a presumption of legitimacy of the processing of medical data. It is assumed that the data subject has correctly assessed the interests in presence and acted accordingly. If the data subject has not correctly assessed the interests in presence and if the interests in presence are not respected, his or her consent will not legitimate the processing of medical data. The latter will not be legitimate on this ground.

28 Directive 95/46/EC, art. 8.2, a) and recital 33.

In other words, the consent of the data subject does not exonerate the data controller from pursuing a legitimate purpose (inducing the balance between the interests in presence) and the consent of the data subject may not cover the illegitimate interest or the lack of interest in the data processing.

15. The Directive provides that the Member States may oppose the possibility for the sole consent of the data subject to lift the prohibition from processing medical data [29].

16. In any case, the data subject may always revoke his or her consent to the processing of medical data. What are the consequences of this revocation?

Does it mean that, for the future, new operations upon the data subject's medical data will not be possible any more (without any effect on the existing data processing) or do we have to consider that the operations realised upon medical data on the ground of the initial consent of the data subject may not be pursued?

Since the data subject has revoked his or her initial consent, there is no more legitimate base for the processing of medical data. The operations may not be pursued. That does not mean that the past operations realised upon the medical data are now unlawful. It simply means that they can not be pursued except on the ground of another base of legitimacy.

17. Finally, the Directive gives no formal indication on the nature of the consent given by the data subject or on the possible contractual relationship between the data controller and the data subject.

In our opinion, the solution to these questions depends on how the applicable law deals with the relationship between the data controller and the data subject and with the relationship between the data subject and personal data. In any case, the possible contract should obey the special rules imposed through the transposition of the Directive in the applicable law such as the characteristics of the data subject's consent, the data quality, the data subject's rights, the security and confidentiality measures, the notification to the supervisory authority, etc.

The applicable law determines also the capacity to consent for underaged or disabled persons.

The Directive provides other solutions to legitimate the processing of medical data.

29 Directive 95/46/EC, art. 8.2, a).

B. Carrying out obligations and specific rights of the data controller in the field of employment law

18. The ban on medical data processing is not applicable when the *"processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorised by national law providing for adequate safeguards"* [30].

First, the purpose of the data processing is to enable the data controller to fulfil his obligations and rights in Employment Law, the latter being specific. This hypothesis seems to include Medical Control.

Then the processing of medical data has to be necessary and not only useful for this purpose. Therefore the data controller has to prove the necessity to process medical data to carry out his obligations and specific rights in the field of Employment Law.

Finally, this kind of processing has to be authorised by the applicable law providing for adequate safeguards, the latter being not further determined.

C. Vital interests

19. The third hypothesis allowing the processing of medical data is when *"processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent"* [31].

The notion of 'vital interest' means expressly and exclusively the situation of an imminent danger to the life of a natural person. This covers the protection of the vital interests of the data subject but also of any other natural person. However, in this last situation, the Directive adds that the data subject must be physically or legally incapable of consenting to the processing of his or her medical data.

It can not be deduced from this disposition that the data subject, physically or legally capable of consenting, could, without any consequence, refuse to authorise the processing of medical data when the vital interests of another person are at stake. The qualification of this behaviour should be qualified under the applicable law.

D. Non-profit organisation

20. The processing of medical data could be legitimate when the *"processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation,*

30 Directive 95/46/EC, art. 8.2, b). See: Data Protection Working Party, Opinion 8/2001 on the processing of personal data in the employment context, WP 48, adopted on 13 Sept. 2001.

31 Directive 95/46/EC, art. 8.2, c).

association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects" [32].

With respect to this, the organisation must have a non-profit purpose relative he exercise of fundamental rights and freedoms.

E. Data manifestly made public and establishment, exercise or defence of legal claims

21. The ban on processing medical data is not applicable when *"the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims"* [33].

It has to be reminded that, even if manifestly made public by the data subject, the processing of sensitive personal data is nevertheless under the scope of the Directive. Hence, the data controller must comply with all the other conditions ensuring the lawfulness of the data processing.

F. Healthcare purpose

22. The ban on medical data processing is not applicable *"where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy"* [34].

The healthcare purpose should be interpreted broadly [35], including the management of healthcare services. The latter should include secondary purposes necessary to provide healthcare such as the welcoming of the patients, medical secretary, computer Department, etc.

By contrast, this hypothesis does not include social security purposes or public health purposes (cf. *infra*).

32 Directive 95/46/EC, art. 8.2, d).
33 Directive 95/46/EC, art. 8.2, e).
34 Directive 95/46/EC, art. 8.3. See: Data Protection Working Party, Working Document on the processing of personal data relating to health in electronic health records, adopted on 15th February 2007, WP 131.
35 However the Directive seems to include only certain purposes relative to healthcare (cf. recital 33).

Medical data must be processed by a health professional, but this last notion has not been further defined. This professional has to be subject under national law or rules established by national competent bodies to professional secrecy.

When not processed by a health professional, the processing may be carried out by another person if he or she is subject to an equivalent obligation of secrecy notably due to his or her status or by way of contractual stipulation or term.

Under this hypothesis, we should question the absence of the consent of the data subject. Has it been mistaken with the consent to the provision of healthcare?

G. Reasons of substantial public interest

23. The Directive grants Member States with permission to lay down additional exemptions for reasons of substantial public interest [36]. Hence, the Member State has to prove in each case the real existence of the considered substantial public interest(s).

The Directive had essentially in mind substantial public interests relative to Public Health and Social Security *"especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system (...)"* [37].

It had also in mind scientific research and public statistics [38].

The cases where medical data may be processed must be laid down by national law or by decision of the supervisory authority.

But Member States may only allow for the processing of medical data if these exceptions are subject to the provision of suitable safeguards to protect the fundamental rights and freedoms of the data subjects and especially their right to respect private life [39].

The Directive does not determine these safeguards.

Member States must notify the exemptions to the ban on processing medical data adopted on this base [40] to the European Commission.

Member States must determine the conditions under which a national identification number or any other identifier of general application may be processed [41].

36 Directive 95/46/EC, art. 8.4.
37 Directive 95/46/EC, recital 34.
38 Directive 95/46/EC, recital 34.
39 Directive 95/46/EC, recital 34.
40 Directive 95/46/EC, art. 8.6.
41 Directive 95/46/EC, art. 8.7.

24. In any case, the legitimacy of the processing of medical data is not complete when only formally fitting into one of these exceptions to the ban on processing medical data, even with the consent of the data subject. Indeed, these exceptions are only hypotheses where the legitimacy of the data processing is formally assumed.

Now the legitimacy of the processing of medical data – the balance of the interests in presence – has to be really assessed.

First, the interests in presence have to be identified. Are they only the interests of the data controller and of the data subject or should we also take into account the interests of third concerned parties and of the whole society? In our view these two last categories of interests should be accounted for when evaluating the legitimacy of the processing of medical data.

Then, the explicit and valid consent of the data subject presumes, until contrary proof, the existence of an acceptable balance between the interests in presence in the processing of medical data. However, in this case, it is quite difficult to assume that the data subject has adequately taken into account interests other than one's own.

In any event, the processing of medical data will not be legitimate if the balance between the interests in presence is not respected, even with the regular consent of the data subject.

25. But the legitimacy of the processing of medical data is definitely and very usefully strengthened by the additional consent of the data subject. That is the reason why we must firmly approve and recommend the ethical practice aiming to obtain the consent of the data subject. This practice is frequent in the conduct of clinical trials and in telematic networks in healthcare.

26. Finally, it has to be stressed that the data controller may not legitimate the processing of medical data on other bases. That excludes necessarily the use of the hypotheses of formal legitimacy enumerated in article 7 of the Directive for non-sensitive personal data. By example, the data controller may not legitimate the processing of medical data by the balance of the interests in presence without meeting the hypotheses enumerated in article 8.

IV. The management of 'specific risks' in the processing of personal data

27. The Directive determines the legal framework applicable in all Member States to the processing of personal data and provides special rules to legitimate the processing of 'sensitive' data. Yet, the Directive considers the situation in which,

without prejudice to this double approach, some processing of personal data may present some specific risks to the data subjects' rights and freedoms [42].

28. In 1995, the Directive has indicated that, regarding any processing of personal data in the society, the cases presenting such specific risks should not be very common [43]. More than ten years later and having in mind the vertiginous evolution of the new information and communication technologies [44], it is not clear that such statement is still valid. By contrast, the number of data processing presenting such specific risks seems nowadays quite significant, especially in healthcare. Indeed, since 1995 the technological evolutions have notably permitted the creation of huge telematic networks linking substantial medical databases and the creation of genetic databases in national or European or worldwide telematic networks. Should we consider that these evolutions have increased the number of data processing presenting specific risks for the data subjects' rights and freedoms?

29. The Directive provides that the specific risks result from the nature of the data processing, from its range or from its purposes [45]. For instance, the Directive cites purposes aiming to exclude persons from the benefit of a right, a service or a contract [46]. These specific risks may also arise from the specific use of a new technology [47]. The latter reminds inevitably the introduction of Grid technologies in healthcare.

Traditionally, the processing of personal data presenting specific risks are those pursued by public authorities and concerning the population (as a whole or in part) or

42 Directive 95/46/EC, recital 53.

43 Directive 95/46/EC, recital 54.

44 To get an idea of the evolution of ICT, see: Council of Europe, T-PD, Report on the application of Convention 108 to the profiling mechanism. Some ideas for the future work of the consultative committee, by J.M. DINANT, C. LAZARO, Y. POULLET, N. LEFEVER et A. ROUVROY, T-PD(2008)01, 11 Jan. 2008; Council of Europe, T-PD, Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data (2005); Council of Europe, Guiding principles for the protection of personal data with regard to smart cards (2004); Council of Europe, T-PD, Report on the application of data protection principles to the worldwide telecommunication networks, by Prof. Y. POULLET and his Team (2004); Council of Europe, Report containing guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance (2003); Council of Europe, T-PD, Report on the protection of personal data with regard to the use of smart cards (2001), by Mr. K. NEUWIRT; Council of Europe, T-PD, Study contracts involving the transfer of personal data between Parties to Convention Ets 108 and third countries not providing an adequate level of protection (2001), by Mr. J. HUET; Council of Europe, T-PD, Protection of personal data with regard to surveillance (2000) and Guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance, by Mr. G. BUTTARELLI.

45 Directive 95/46/EC, recital 53.

46 See: Data Protection Working Party, Working Document on Blacklists, WP 65, adopted on 3 Oct. 2002 and C. BURTON & Y. POULLET, "A propos de l'avis de la Commission de la protection de la vie privée du 15 juin 2005 sur l'encadrement des listes noires", note d'observations, *Revue du droit des technologies de l'information*, Brussels, Ed. Bruylant, n° 23, 2005, p. 79-122.

47 Directive 95/46/EC, recital 53.

those concerning medical data [48]. Genetic databases and telematic networks in healthcare are further examples of data processing susceptible to present specific risks to the data subjects' rights and freedoms. One should pay attention to the person of the data controller [49], to the sensitivity of the processed data, to the purposes of the data processing, to the range of the data processing, to the categories of data subjects and to the respect of their rights, keeping in mind the transfer of the personal data outside Europe. In short, one should beware of anything that could create specific risks to the data subjects' rights and freedoms. But any processing of sensitive data does not necessarily present specific risks and the processing of 'ordinary' personal data should not be *a priori* excluded as it may also present specific risks to the data subjects' rights and freedoms.

30. Regarding the development of the telematic networks in healthcare, the specific risks result primarily from the fact that medical data may be processed for multiple purposes. This raises the question whether it is permissible to process medical data for multiple purposes. This also raises the issue of the prior determination of the precise and real purposes of the data processing. In addition, appears the question of further data processing. Indeed, the actual trend aims to not determine anymore on a prior and precise way the purposes of the data processing, but to organise an entire information system combined with a security system in which the data processing purposes will be determined later. Put differently, we witness today the creation of an information system with two levels. First, the infrastructure of the information system is created, implying in some extent the collection and the processing of personal data in a virtual complex (notably to identify the actors of the information system – mainly the patients and the health practitioners). Only then, the purposes permitted by the infrastructure are determined, forgetting that these purposes rely on an initial data processing (the creation of the first level of the information system (its infrastructure)). Doing so, the creation of the first level of the information system does not seem to constitute such a risk to the data subjects' rights and freedoms even when this first level is at the origin of the risks. But both the first (the creation of the infrastructure or the network) and further data processing permitted by the infrastructure of the information system have to be assessed. And if the security level helps to assess (and to reduce) the risks induced by the data processing, it does not prevent to take into account the other criteria to legitimate the data processing (for both levels of the information system), especially when the processing concerns sensitive data such as medical or genetic data.

[48] Y. POULLET, M.-H. BOULANGER, C. de TERWANGNE, Th. LEONARD, S. LOUVEAUX, & D. MOREAU, o.c., *Journal des Tribunaux de Droit Européen*, Brussels, Larcier, 1997, p. 152, n° 62.

[49] E.g. a commercial company processing medical or genetic data.

These new information systems are part of a structural policy aiming at building telematic networks (information highways) in healthcare. They also indicate the transition from a vertical conception of e-Health to a new conception which is, in a first step, abstract, horizontal and transversal (the infrastructure of the information system) and which becomes, in a second step, vertical and real (the applications – e-Health products and services – using the infrastructure). The mere existence of these new telematic infrastructures in healthcare enables to share scientific databases but implies the identification of the practitioners and patients through special registries, etc. Eventually, these telematic networks will deeply modify the organisation of the public health systems and all actors in healthcare will be concerned and involved: practitioners, patients, institutions and bodies in healthcare and social security, medical laboratories, etc.

But once again, these new information systems differ in their permanency, irrespective of their future applications. Hence, the opportunity to create these infrastructures is no more evaluated regarding their precise and real purposes. Their opportunity is assessed in an abstract way with respect to some categories of purposes whose precise and real content will be determined later. This constitutes a deep change in the required precision and reality to evaluate the purposes pursued by the creation of the telematic infrastructure and its future exploitation.

These new information systems with multiple levels and purposes pose problems regarding the fairness of the data processing since this requires to respect the precise and real purposes announced at the beginning of the data processing. It also poses problems with respect to the duty to properly inform the data subject. Indeed, the multiple ramifications of the information system are not transparent, regarding both the technical level as well as the purposes of the data processing ('black box' issue).

However, it must be said that the new information and communication technologies should be able to address properly all these issues.

V. Consequences of the presence of 'specific risks' in the processing of personal data

31. Member States have a duty to identify the processing of personal data likely to present specific risks to the data subjects' rights and freedoms and to take appropriate measures to ensure the prior checking of the processing of personal data before their starting [50].

The fact that medical data are already subject to special rules due to their sensitive nature does not exclude them from the scope of additional rules relative to data

[50] Directive 95/46/EC, art. 20.1.

processing presenting specific risks. In other words, the processing of medical data presenting specific risks for the data subjects' rights and freedoms has to be checked prior its beginning. However, any medical data processing does not automatically present specific risks. And processing of 'ordinary' personal data may also arouse specific risks.

32. The prior checking of data processing presenting specific risks may take place via four different ways.

Firstly, the prior checking may be carried out by the national supervisory authority following receipt of the notification from the data controller [51]. The national supervisory authority may, according to the applicable national law, issue an opinion or authorise the data processing [52].

Secondly, the prior checking may be realized by the data protection official [53]. In case of doubt, this person has to consult the national supervisory authority [54]. With respect to this, the Directive indicates that the data protection official will proceed in cooperation with the national supervisory authority [55].

Thirdly, the Directive provides that Member States may carry out the prior checking in the context of the preparation of a measure of the national parliament, which defines the nature of the data processing and lies down appropriate safeguards [56].

Fourthly, Member States may also realize to this prior checking in the context of the preparation of a measure based on a legislative measure, which defines the nature of the data processing and lies down appropriate safeguards [57].

51 Directive 95/46/EC, art. 20.2.

52 Directive 95/46/EC, recital 54.

53 The personal data protection official is a person appointed by the data controller in compliance with the national law which governs him. This official is responsible in particular:
- for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive,
- for keeping the register of processing operations carried out by the controller, containing the items of information referred to in article 21.2,

thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations (Directive 95/46/EC, art. 18.2).
The presence of a data protection official allows Member States to provide for the simplification of or the exemption from the notification duty (Directive 95/46/EC, art. 18.2).

54 Directive 95/46/EC, art. 20.2.

55 Directive 95/46/EC, recital 54.

56 Directive 95/46/EC, art. 20.3.

57 Directive 95/46/EC, art. 20.3.

VI. 'Specific risks' in the processing of personal data and the use of Healthgrid technologies

33. Beyond the mere question of the legitimacy of the medical data processing, it is now possible to know whether the use of Healthgrid technologies may induce 'specific risks' with regard to data protection. This question is exclusively focused on the use of such technologies and not on the outlines of its implementation project. What could lead to the conclusion that the use of Healthgrid technologies may induce such specific risks?

a) The phenomenal storage capacities of Healthgrid technologies are of nature to cause specific risks with regard to data protection. In this case, specific risks may result from the storage of an important amount of personal data. More stored data mean more risks. Naturally, the risk is increased in the presence of sensitive data.

b) The extraordinary capacities of Healthgrid technologies to process a huge amount of personal data widely disseminated may also open the door to specific risks with regard to data protection. More operations upon personal data mean more risks. Again, the risk is greater in the case of sensitive data.

c) The size of the Healthgrid information system has to be considered, including its inscription in a broad European or international network: the larger, the riskier.

d) A specific risk could result from the data subjects' instrumentalisation as they could appear more as informational sources than as patients. It could also lead to discriminations in the provision of healthcare or medicines or treatment or diagnosis.

e) The duration of the Healthgrid information system could also create specific risks to data protection (the 'eternity effect').

f) The use of Healthgrid technologies by public authorities or bodies should be considered as inducing specific risks towards data protection.

g) If the exercise of data subjects' rights is more difficult due to the use of Healthgrid technologies, it should be recognised as a specific risk to data protection.

h) Generally, the use of Grid technologies implies the transfer of personal data outside Europe. The complexity of this kind of information system could lead to acknowledge the presence of specific risks towards data protection.

These criteria may naturally be combined, increasing therefore the risks for data subjects' rights and freedoms.

When considering the specific risks that may emerge with the introduction of Healthgrid technologies in healthcare, one should not forget to take into account the benefits of its use.

But again, it must be stressed that the new information and communication technologies could help to address these issues.

VII. Conclusions

34. This paper investigates the management by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, of the risks related to the underlying processing of medical data occurring in Healthgrids.

We have demonstrated that the risk management in the processing of personal data is deployed in four steps.

Firstly, in principle, risks are assessed regarding the purposes of the data processing and do not depend on the informational content of the processed personal data.

Secondly, this principle is slightly though not completely different for sensitive data. For them, risks are assessed regarding their informational content as well as the purposes of their processing.

Thirdly, data processing presenting specific risks for data subjects' rights and freedoms must be subject to a prior checking beforehand. The checking may take place in four different ways.

Fourthly, transfers of personal data outside Europe are ruled by special rules.

35. We have shown that regarding their highly sensitive nature, medical data require a special protection taking into account their informational content and the purpose of their processing. Therefore, Directive 95/46/EC has decided to prohibit the processing of medical data. However, the Directive provides that this ban does not apply in seven cases. These exceptions to the ban on processing medical data have to be restrictively interpreted. In these cases, the legitimacy of the processing of medical data is formally assumed without prejudice for the other conditions ensuring the lawfulness of the data processing.

36. The explicit and valid consent of the data subject constitutes the very first source of legitimacy for the processing of medical data even if, at the same time, it might be the weakest base to legitimate the processing of medical data due to the strict conditions on its validity and to the possibility for the data subject to revoke

his or her consent at any time and without justification (but with reasonable notice in some cases?).

Nevertheless, even if the data controller may legitimate the processing of medical data with the consent of the data subject, the legitimacy of the data processing must be really assessed in each case by the balance of the interests in presence. These include the interests of the data subject, of the data controller, of the third concerned parties and of the society.

In any case, the consent of the data subject may not cover the lack of legitimacy or the illegitimacy of the processing of medical data. The consent of the data subject only creates the presumption of legitimacy of the processing of medical data until proof of the contrary, as do the other exceptions to the ban on processing medical data.

We should approve and recommend very strongly and warmly the ethical practice requiring the consent of the data subject when processing medical data, even if the latter might rely on another base of legitimacy.

37. Due to some of its characteristics, the use of Healthgrid technologies in healthcare could induce specific risks with regard to data protection.

This issue should be carefully monitored by the data controller as well as by the national supervisory authorities.

In these situations, it seems more than appropriate to appoint a personal data protection official to the benefit of everyone in terms of legitimacy, transparency, data subjects' rights and freedoms, confidentiality, security and efficiency.

Finally, these specific risks should not prevent the use of Grid Technologies in healthcare notably due to their potential but extraordinary benefits for knowledge and healthcare. They should only lead to the adoption of appropriate measures as previously described in order to ensure the respect of data subjects' rights and freedoms to which the entire Healthgrid Community is deeply committed.

SELECTIVE BIBLIOGRAPHY

BENNETT, B. (ed.), *e-Health Business and Transactional Law*, Washington, BNA Books, 2002, 734 p.

BEYLEVELD, D., TOWNEND, D., ROUILLE-MIRZA, S. & WRIGHT, J. (ed.), *Implementation of the Data Protection Directive in relation to Medical Research in Europe*, Ashgate Publishing, 2004.

BEYLEVELD, D., TOWNEND, D., ROUILLE-MIRZA, S. & WRIGHT, J. (ed.), *The Data Protection Directive and Medical Research across Europe*, Ashgate Publishing, 2005.

BEYLEVELD, D., TOWNEND, D. & WRIGHT, J. (ed.), *Research Ethics Committees, Data Protection and Medical Research in European Countries*, Ashgate Publishing, 2005.

BEYLEVELD, D., TOWNEND, D. & WRIGHT, J. (ed.), *Research Ethics Committees, Data Protection and Medical Research in Europe*, Ashgate Publishing, 2007.

BURTON, C. & POULLET, Y., "A propos de l'avis de la Commission de la protection de la vie privée du 15 juin 2005 sur l'encadrement des listes noires", note d'observations, *Revue du droit des technologies de l'information*, Brussels, Ed. Bruylant, n° 23, 2005, p. 79-122.

BOULANGER, M.-H., DE TERWANGNE, C., LEONARD, Th., LOUVEAUX, S., MOREAU, D. & POULLET, Y., "La protection des données à caractère personnel en droit européen", *Journal des Tribunaux de Droit Européen*, Bruxelles, Larcier, 1997, p. 121 (en trois parties).

CALLENS, S. & HEERDT, J., "Juridische beschouwingen bij telegeneeskunde", *Revue de Droit de la Santé*, Mys & Breesch, 1999-2000, p. 310.

CALLENS, S. (ed.), *e-Health and the Law*, The Hague, Kluwer Law International, 2003, 183 p.

CHABERT-PELTAT, C., "La télémédecine", *Revue Alain Bensoussan – Droit des Technologies Avancées*, Paris, 1999, n° 6/3-4, p. 117-138.

Commission nationale de l'informatique et des libertés (CNIL-France), Délibération n° 97-049 du 24 juin 1997 portant avis sur la mise en œuvre à titre expérimental d'un réseau de télémédecine sur Internet entre le Centre hospitalier d'Annecy et certains médecins de ville, Revue Alain Bensoussan – Droit des Technologies Avancées, Paris, 1999, n° 6/3-4, p. 169-172.

DE BOT, D., *Verwerking van persoongegevens*, Kluwer, 2001.

DE CLIPPELE, Fr., "The Law on e-Health: Draft Proposal for an Electronic Medical Prescription", *Acta Chir. Belg.*, n° 105, 2005, p. 450-454.

DE TERWANGNE, C., "Affaire Lindqvist ou quand la Cour de justice des Communautés européennes prend position en matière de protection des données personnelles", obs. sous C.J.C.E, arrêt du 6 nov. 2003, Bodil Lindqvist, affaire C-101/01, *Revue du droit des technologies de l'information*, Bruxelles, Ed. Bruylant, 2004, p. 67-99.

DUQUENOY, P., GEORGE, C. & KIMPPA, K., *Ethical, Legal and Social Issues in Medical Informatics*, (to be published in 2008).

FLEISHER, L.D. & DECHENE, J.C., *Telemedicine and e-Health Law*, Law Journal Press, 2004.

HERVEG, J., "Healthgrid from a Legal Point of View", in *From GRID to HEALTHGRID*, Studies in Health Technology and Informatics, Volume 112, part 5, IOS Publications, 2005, p. 312-318.

HERVEG, J., "The Ban on Processing Medical Data in European Law: Consent and Alternative Solutions to Legitimate Processing of Medical Data in HealthGrid", in *Challenges and Opportunities of HealthGrids*, Studies in Health Technology and Informatics, Volume 120, IOS Press, 2006, p. 107-116.

HERVEG, J., "La gestion des risques spécifiques aux traitements de données médicales en droit européen", in *Systèmes de santé et circulation de l'information, Encadrement éthique et juridique*, Paris, Dalloz, 2006, p. 79-103.

HERVEG, J., "La protection des données médicales en droit européen", in *Dossier médical et données médicales de santé: Protection de la confidentialité, conditions d'accès, échanges pour les soins et la recherche*, Bordeaux, Ed. Les études hospitalières, 2007, p. 183-196.

HERVEG, J., "Does HealthGrid Present Specific Risks With Regard To Data Protection?", in *From Genes to Personalized HealthCare: Grid Solutions for the Life Sciences*, IOS Publications, Studies in Health Technology and Informatics, 2007, vol. 126, p. 219-228.

HERVEG, J., "Confidentialité et sécurité pour les applications de télémédecine en droit européen", in *Lex Electronica*, 2007, vol. 12, issue 1.

HERVEG, J. et POULLET, Y., « Legal approaches of the HealthGrid technology », in *Healthgrid - White Paper*, Healthgrid Association, 2004.

HERVEG, J. et POULLET, Y., "Which Major Legal Concerns in Future eHealth?", in *The Information Society: Innovation, Legitimacy, Ethics and Democracy in Honor of Professor Jacques Berleur s.j.*, Boston, Springer, International Federation for Information Processing (IFIP), 2007, vol. 233, p. 159-170.

HERVEG, J. & VAN GYSEGHEM, J.-M., "La sous-traitance des données du patient au regard de la directive 95/46", *Lex Electronica*, vol. 9, n° 3, t. 2004, http://www.lex-electronica.org/articles/v9-3/herveg_vangyseghem.htm.

HERVEG, J., VAN GYSEGHEM, J.-M. & DE TERWANGNE, C., *GRID-enabled medical simulation services and European Law, Final Report on all the Legal Issues related to Running GRID Medical Services*, European Research contract IST-2001-37153-GEMSS, 29 February 2005, 341 p.

HERVEG, J., VERHAEGEN, M.-N. & Y. POULLET, "Les droits du patient face au traitement informatisé de ses données dans une finalité thérapeutique: les conditions d'une alliance entre informatique, vie privée et santé", *Revue de Droit de la Santé*, Kluwer, 2002-2003/2, p. 56-84.

IAKOVIDIS, I., WILSON, P., Healy, J.-Cl., *E-Health: Current Situation and Examples of Implemented and Beneficial E-Health Applications*, Studies in Health Technology and Informatics, Volume 100, IOS Press, 2004, 249 p.

KAPLAN, G. & MCFARQUHAR, E., *e-Health Law Manual*, New-York, Aspen Publishers, 2003.

MIDDLETON, S.E., HERVEG, J., CRAZZOLARA, F., MARVIN, D. & POULLET, Y., "GEMSS: Security and Privacy for a Medical Grid", *Methods of Information in Medicine*, Verlag für Medizin und Naturwissenschaften, Stuttgart, Schattaeur, 2005, 44/2, p. 182-185.

OLIVE, M., RAHMOUNI, H., SOLOMONIDES, T., BRETON, V., LEGRE, Y., BLANQUER, I., HERNANDEZ, V., ANDOULSI, I., HERVEG, J. et WILSON, P., "SHARE Roadmap 1: Towards a debate", in *From Genes to Personalized HealthCare: Grid Solutions for the Life Sciences*, Studies in Health Technology and Informatics, vol. 126, IOS Publications, 2007, p. 164-173.

RIENHOFF, O., LASKE, C., VAN EECKE, P., WENZLAFF, P. & PICCOLO, U., *A Legal Framework for Security in European Health Care Telematics*, Amsterdam, IOS Press, Studies in Health Technology and Informatics, 2000, vol. 74, 202 p.

RIGAUX, Fr., *La protection de la vie privée et des autres biens de la personnalité*, Bruxelles, Paris, Bruylant, L.G.D.J., 1990.

RODRIGUES, R.J., WILSON, P. & SCHANZ, S.J., *The Regulation of Privacy and Data Protection in the Use of Electronic Health Information, An International Perspective and Reference Source on Regulatory and Legal Issues Related to Person-Identifiable Health Databases*, Pan American Health Information, World Health Organisation, 2001, 217 p.

ROGER-FRANCE, Fr., "Informations de santé, télématique et télémédecine, Perspectives d'ensemble à l'horizon 2000", *Journal de réflexion sur l'informatique*, 1994, n° 30, p. 7-9.

ROUSSEAU, A. & HERVEG, J., *Manuel d'informatisation des urgences hospitalières*, Louvain-la-Neuve, Presses Universitaires de Louvain, 2003, 183 p.

SCHAMPS, G., "L'établissement d'un diagnostic à distance et la responsabilité médicale", *Revue de Droit de la Santé*, Mys & Breesch, 1996-1997, p. 8 et s.

SILBER, D., *The case for eHealth*, Maastricht, Institut Européen d'Administration Publique (ed.), 2003, 32 p.

STANBERRY, B., *The Legal and Ethical Aspects of Telemedicine*, London, Royal Society of Medicine Press, 1998, 172 p.

VAN DOSSELAERE, C., HERVEG, J., SILBER, D. & WILSON, P., *Legally and regulatory aspects of e-Health – Putting e-Health in its European Legal Context, European Commission, DG Information Society and Media*, Study report, March 2008.

VAN EECKE, P., "Electronic Health Care Services and the e-Commerce Directive", in *A decade of research @ the crossroads of law and ICT*, Gent, Larcier, 2001, p. 365-379.

VILCHES ARMESTO, L., "IMS Health: dernier développement de la C.J.C.E. relatif au refus de licence en droit de propriété intellectuelle", note sous C.J.C.E., 29 avril 2004, *Revue du Droit des Technologies de l'Information*, Brussels, Larcier, 2004, n° 20, p. 59 et s.

WILSON, P., LEITNER, Chr. & MOUSSALI, A., *Mapping the Potential of e-Health, Empowering the citizen through e-Health tools and services*, Maastricht, European Institute of Public Administration (ed.), 2004, 52 p.